AMENDMENTS TO THE CLAIMS:

This listing of the claims will replace all prior versions, and listings, of the claims in this application.

Listing of Claims:

1.-13.(Canceled)

14.(Previously Presented) A method, comprising:

extracting, at a network element, routing information from a received message at a border between a first network and a second network;

generating a decrypted and reversed routing information by decrypting a tokenized second-network routing entry relating to a routing path of said message within said second network and by reversing the content of the decrypted second-network routing entry;

replacing said routing information of said received message by said decrypted and reversed routing information;

forwarding said received message with said decrypted and reversed routing information to said second network;

marking a tokenized network routing entry of at least one of an incoming and outgoing tokenized network node; and

performing at least one of suppressing said reversing at outgoing tokenizing network nodes and reversing network routing entries at incoming tokenizing network nodes before encryption.

15.(Previously Presented) The method according to claim 14, further comprising:

conveying said routing information in a routing header of said message.

16.(Previously Presented) The method according to claim 15, wherein said routing header comprises at least one of a route header and a via header of a session initiation protocol message.

17.(Currently Amended) The method according to [[any]] claim 14, further comprising:

using a topology hiding method.

18.(Previously Presented) The method according to claim 17, further comprising applying said topology hiding method in response to a user identity marked with a predetermined information.

19.(Previously Presented) The method according to claim 17, further comprising

applying said topology hiding method in response to a network identity.

20.(Previously Presented) The method according to claim 14, wherein said tokenized second-network routing entry comprises at least one of an encrypted name and encrypted address information of a sequence of network nodes through which said received message has been routed.

21.(Canceled)

22.(Canceled)

23.(Previously Presented) The method according to claim 14, wherein said border between said first and second networks is defined at a gateway device which said message traverses on a connection between said first and second networks.

24.(Previously Presented) An apparatus, comprising:

extracting means for extracting routing information from a received message at a border between a first network and a second network;

decrypting and reversing means for generating a decrypted and reversed routing information by decrypting a tokenized second-network routing entry relating to a routing path of said message within said second network and by reversing the content of the decrypted second-network routing entry;

replacing means for replacing said routing information of said received

message by said decrypted and reversed routing information;

forwarding means for forwarding said received message with said decrypted and reversed routing information to said second network;

marking means for marking a tokenized network routing entry of at least one of an incoming and an outgoing tokenizing network node; and

at least one of suppressing means for suppressing said reversing at outgoing tokenizing network nodes and reversing means for reversing network routing entries at incoming tokenizing network nodes before encryption.

25.(Previously Presented) The apparatus according to claim 24, further comprising one of an interrogating call session control function and a topology hiding gateway function.

26.(Previously Presented) The apparatus according to claim 24, wherein said apparatus operates in a packet data network which comprises an Internet protocol multimedia subsystem.

27.(Previously Presented) The apparatus according to claim 24, wherein said apparatus is configured to suppress reversing of said decryptor and reverser when said routing information indicates that said apparatus is an outgoing tokenizing network node.

28.(Previously Presented) The apparatus according to claim 24, wherein said apparatus is configured to reverse network routing entries before encryption when said routing information indicates that said apparatus is an incoming tokenizing apparatus.

29.(Previously Presented) The apparatus according to claim 24, wherein said border between said first and second networks is defined at said apparatus.

30.(Canceled)

31.(Previously Presented) An apparatus, comprising:

an extractor configured to extract a routing information from a received message at a border between a first network and a second network;

a decryptor, operably connected to said extractor, and configured to generate a decrypted and reversed routing information by decrypting a tokenized second-network routing entry relating to a routing path of said message within said second network and further configured to reverse the content of the decrypted second-network routing entry;

a replacer, operably connected to said extractor, and configured to replace said

routing information of said received message with said decrypted and reversed routing information;

a transmitter, operably connected to said extractor, and configured to forward said received message with said decrypted and reversed routing information to said second network;

a marker configured to mark a tokenized network entry of at least one of an incoming and an outgoing tokenizing network node; and

a processor configured to perform at least one of suppressing said reversing at outgoing tokenizing network nodes and reversing network entries at incoming tokenizing network nodes before encryption.

32.(Previously Presented) The apparatus according to claim 31, further comprising:

one of an interrogating call session control function and a topology hiding gateway function.

33.(Previously Presented) The apparatus according to claim 31, wherein said apparatus operates in a packet data network which comprises an Internet protocol (IP) multimedia subsystem.

34.(Previously Presented) The apparatus according to claim 31,

wherein said apparatus is configured to suppress reversing of said decrypter when said routing information indicates that said apparatus is an outgoing tokenizing apparatus.

35.(Previously Presented) The apparatus according to claim 31, wherein said apparatus is configured to reverse network routing entries before encryption when said routing information indicates that said apparatus is an incoming tokenizing apparatus.

36.(Previously Presented) The apparatus according to claim 31, wherein said border between said first and second networks is defined at said apparatus.

37.-39.(Canceled)